The Claims

1. (Previously presented) A multi-tiered management architecture comprising:

an application development tier at which applications are developed for execution on one or more computers;

an application operations tier at which execution of the applications is managed; and

a cluster operations tier to manage the operation of the computers without concern for what applications are executing on the one or more computers, wherein the cluster operations tier is responsible for securing a computer cluster boundary to prevent a plurality of other computers that are not part of the computer cluster from accessing the one or more computers in the computer cluster.

2. (Canceled).

3. (Previously presented) A management architecture as recited in claim 1, wherein the application operations tier is responsible for securing sub-boundaries within the computer cluster boundary to restrict communication between computers within the computer cluster.

4. (Original) A management architecture as recited in claim 1, wherein the application operations tier is implemented at an application operations management console at a location remote from the one or more computers.

5. (Original) A management architecture as recited in claim 1, wherein the cluster operations tier is implemented at a cluster operations management console located at the same location as the one or more computers.

6. (Original) A management architecture as recited in claim 1, wherein the application operations tier monitors execution of application processes on the one or more computers and detects failures of the application processes.

7. (Original) A management architecture as recited in claim 1, wherein the application operations tier takes corrective action in response to a software failure on one of the computers.

8. (Original) A management architecture as recited in claim 7, wherein the corrective action comprises re-booting the computer.

9. (Original) A management architecture as recited in claim 7, wherein the corrective action comprises notifying an administrator of the failure.

10. (Original) A management architecture as recited in claim 1, wherein the cluster operations tier monitors hardware operation of the one or more computers and detects failures of the hardware.

11. (Original) A management architecture as recited in claim 1, wherein the cluster operations tier takes corrective action in response to a hardware failure of one of the computers.

12. (Original) A management architecture as recited in claim 11, wherein the corrective action comprises re-booting the computer.

13. (Original) A management architecture as recited in claim 11, wherein the corrective action comprises notifying a co-location facility administrator.

14. (Original) A management architecture as recited in claim 11, wherein the one or more computers are situated in one or more clusters at a co-location facility.

15. (Currently amended) A co-location facility system comprising:

a plurality of server node clusters, each cluster corresponding to a different customer, where each server node comprises a management component that regulates network communication between the server nodes in accordance with network filters received from one or more cluster operations management consoles

and in accordance with network filters received from remote consoles of the customers, where the management components give precedence to network filters from the one or more cluster operations management consoles over the network filters from the remote consoles such that network filters from the remote consoles cannot enable communications between applications on server nodes across cluster boundaries that have been defined by the network filters received from the one or more cluster operations management consoles; and

[[a]] the one or more cluster operations management consoles corresponding to ~~at least~~ one or more of the server node clusters and configured to manage hardware operations of the ~~at least~~ one or more server node clusters.

16. (Currently amended) A system as recited in claim 15, further comprising a different cluster operations management console corresponding to each of the plurality of server node clusters.

17. (Currently amended) A system as recited in claim 15, wherein each of the plurality of server node clusters includes, as its server nodes, a plurality of server computers.

18. (Original) A system as recited in claim 15, wherein the hardware operations include one or more of: mass storage device operation, memory device operation, and network interface operation, and processor operation.

19. (Currently amended) A system as recited in claim 15, wherein each management console is ~~of the plurality of node clusters includes a plurality of nodes~~ configured to receive node control commands from an application operations management console located remotely from the co-location facility.

20. (Currently amended) A system as recited in claim 19, wherein each server node in each server node cluster is configured with a private key that allows the server node to decrypt communications that are received, in a form encrypted using a public key, from the application operations management console associated with the customer that corresponds to the node cluster.

21. (Currently amended) A system as recited in claim 15, further comprising a data transport medium coupled to each server node in the plurality of server node clusters via which each node can access an external network.

22. (Original) A system as recited in claim 15, wherein the external network comprises the Internet.

23. (Currently amended) A system as recited in claim 15, wherein each server node in each server node cluster is configured with the boundary of the server node cluster.

24. (Currently amended) A system as recited in claim 15, wherein each server node in each server node cluster is configured with a private key that allows the server node to decrypt communications that are received, in a form encrypted using a public key, from at least one of the one or more cluster operations management consoles.

25. (Currently amended) A system as recited in claim 15, wherein one or more of the server nodes in a server node cluster are leased by the customer from an operator of the co-location facility.

26-73 (Canceled).

73. (Currently amended) A multi-tiered computer management architecture comprising:

a first tier corresponding to an owner or lessee of a computer;

a second tier, implemented by a cluster operations management console, corresponding to a hardware operator that is to manage hardware operations of the computer but not application software operations of the computer;

a third tier, implemented by an application operations management console, corresponding to a software operator that is to manage software application operations of the computer but not hardware operations of the computer; and

a fourth tier corresponding to the owner or lessee, wherein the owner or lessee operates in the fourth tier except when revoking ~~the~~ rights of the hardware operator or software operator.

74. (Currently amended) An architecture as recited in claim 73, wherein the ~~second tier management is implemented at a~~ cluster operations management console is at a location remote from the computer.

75. (Currently amended) An architecture as recited in claim 73, wherein the ~~third tier management is implemented at a~~ application operations management console is at a location remote from the computer.

76. (Currently amended) An architecture as recited in claim 73, further comprising using a plurality of key pairs, each key pair including a private key and a public key, to securely communicate between the computer and [[a]] the cluster operations management console ~~device corresponding to the hardware operator~~, as well as between the computer and [[a]] the application operations management console ~~device corresponding to the software operator~~.

77. (Currently amended) A system as recited in claim 15, wherein the one or more cluster operations management consoles [[is]] are configured to manage hardware operations of the ~~at least~~ one or more server node clusters without concern for what applications are executing on server nodes of the server node cluster, and wherein the one or more server cluster operations management consoles [[is]] are responsible for securing a server node cluster boundary to prevent a plurality of other server nodes that are not part of the at least one server

node cluster from accessing the server nodes of the at least one server node cluster.